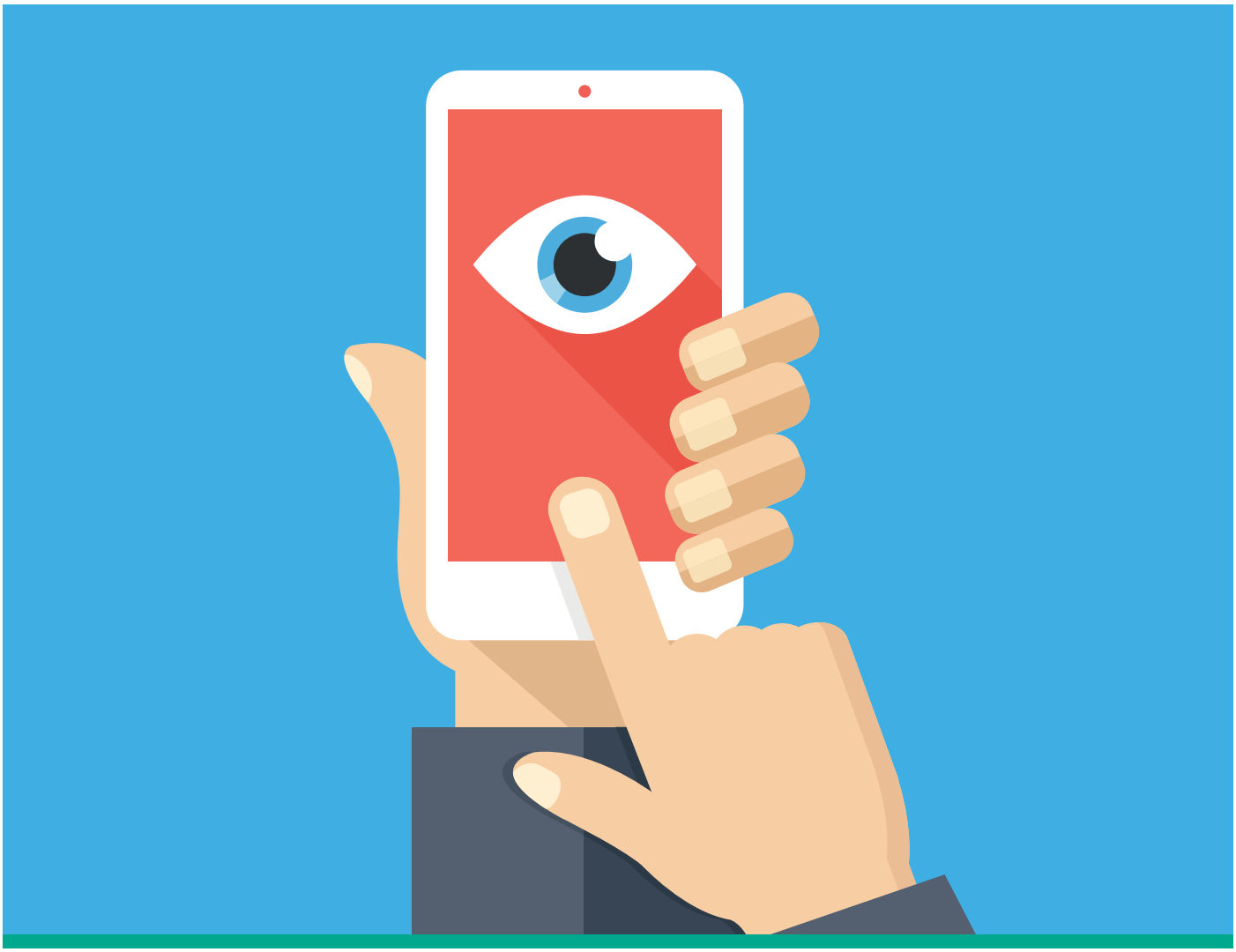


Der **Stalkerware** Report 2020

COALITION AGAINST STALKERWARE

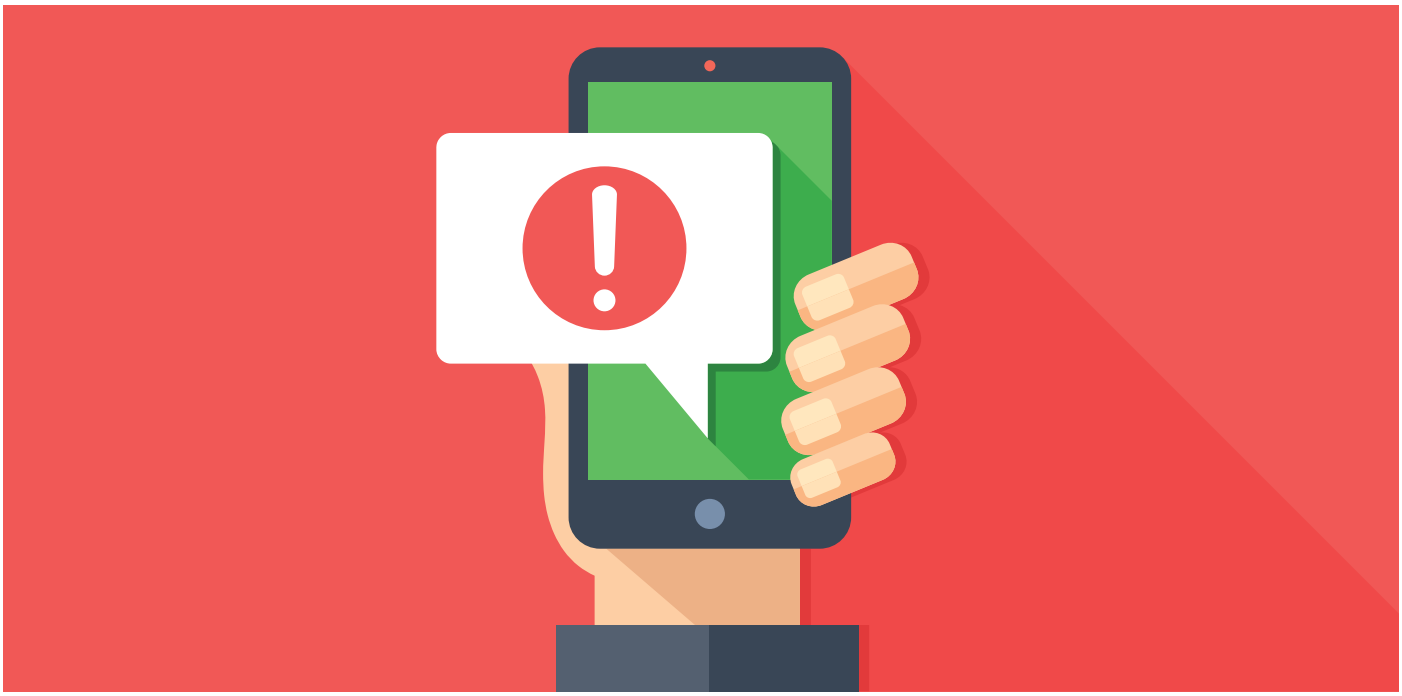
kaspersky

Inhalt

Zentrale Erkenntnisse für 2020

Die Daten von Kaspersky zeigen, dass sich das Ausmaß des Stalkerware-Problems im Jahr 2020 im Vergleich zum Vorjahr nicht wesentlich verbessert hat:

- Die Anzahl der betroffenen Personen ist nach wie vor hoch. Insgesamt waren im Jahr 2020 weltweit 53.870 unserer Mobile User von Stalkerware betroffen. Wenn man das Gesamtbild betrachtet, dürfte die Anzahl weltweit noch weitaus höher liegen, denn unsere Zahlen beziehen sich nur auf Nutzer von Kaspersky-Produkten. Manche betroffenen Nutzer haben möglicherweise eine andere Cybersicherheitslösung auf ihren Geräten installiert, während andere überhaupt keine Lösung verwenden.
- Mit mehr als 8.100 betroffenen Nutzern weltweit ist Nidb laut unserer Statistik für 2020 das am häufigsten verwendete Stalkerware-Programm. Dieses Programm wird verwendet, um eine Reihe von verschiedenen Stalkerware-Produkten zu verkaufen, wie z. B. iSpyoo, TheTruthSpy und Copy9.
- Bezüglich der geografischen Verteilung zeichnet sich ein weitgehend konstanter Trend ab: Russland, Brasilien und die USA bleiben die am stärksten betroffenen Länder weltweit und stehen im Jahr 2020 erneut an der Spitze.
- In Europa sind Deutschland, Italien und das Vereinigte Königreich (UK) am stärksten betroffen.



Einführung und Methodik

Dank heutiger Technologie können wir uns mehr als je zuvor miteinander vernetzen. Wir können unser Leben unabhängig von räumlicher Entfernung digital mit unseren Partnern, unserer Familie und unseren Freunden teilen. Damit einher geht jedoch auch eine Zunahme von Software, die es jemandem ermöglicht, das Leben einer anderen Person aus der Ferne auszuspionieren, ohne dass die betroffene Person ihre Einwilligung dazu erteilt oder dies bemerkt.

Die Risiken von Stalkerware können dabei über die digitale Sphäre hinausgehen und in das reale Leben übergehen. Die Koalition gegen Stalkerware warnt, dass Stalkerware „die Überwachung von Intimpartnern, Belästigung, Missbrauch, Stalking und/oder Gewalt erleichtern kann".

Diese als Stalkerware bekannte Software ist für jeden, der Zugang zum Internet hat, frei zugänglich und zu erwerben. Die Risiken von Stalkerware können dabei über die digitale Sphäre hinausgehen und in das reale Leben übergehen. Die Koalition gegen Stalkerware warnt, dass Stalkerware „die Überwachung von Intimpartnern, Belästigung, Missbrauch, Stalking und/oder Gewalt erleichtern kann". Da Stalkerware im Tarnmodus arbeitet, heißt das, dass sie nicht in Form eines Symbols auf dem Gerät angezeigt wird und für die betroffene Person nicht sichtbar ist. Die Mehrheit der betroffenen Nutzer weiß nicht einmal, dass diese Art von Software existiert. Das bedeutet, dass sie sich weder online noch offline schützen können, zumal die Täter ihre Opfer meist persönlich kennen.

In den letzten Jahren hat Kaspersky aktiv mit Partnern zusammengearbeitet, um die Ausbreitung und Verwendung von Stalkerware zurückzudrängen. Im Jahr 2019 haben wir ein spezielle Warnmeldung entwickelt, die Nutzer benachrichtigt, wenn Stalkerware auf ihren Smartphones installiert ist. Außerdem sind wir eines von zehn Gründungsmitgliedern der Koalition gegen Stalkerware (Coalition Against Stalkerware, CAS). Im selben Jahr veröffentlichten wir auch unseren ersten vollständigen Bericht über Stalkerware, um das Ausmaß des Problems zu verdeutlichen.

Der vorliegende Bericht setzt unsere Untersuchungen zum Thema Stalkerware fort und präsentiert neue Statistiken aus dem Jahr 2020 im Vergleich zu unseren früheren Daten. Die Daten in diesem Bericht stammen aus aggregierten Bedrohungsstatistiken, die aus dem Kaspersky Security Network gewonnen wurden. Das Kaspersky Security Network verarbeitet für Cybersicherheit relevante Datenströme von Millionen freiwilligen Teilnehmern aus aller Welt. Alle empfangenen Daten werden anonymisiert. Zur Berechnung unserer Statistik betrachten wir den Verbraucherstrang der mobilen Sicherheitslösungen von Kaspersky.

Das Problem der Stalkerware und die Hintergründe

Stalkerware ist für jeden, der Zugang zum Internet hat, frei beziehungsweise kommerziell verfügbar. Sie dient der Ausspionierung einer anderen Person aus der Ferne über deren Gerät, ohne dass diese betroffene Person ihre Einwilligung erteilt oder davon erfährt. Stalkerware arbeitet im Tarnmodus. Das bedeutet, dass ihr Vorhandensein nicht durch ein Icon auf dem Gerät angezeigt wird – sie bleibt für die betroffene Person unsichtbar. Deshalb wird Stalkerware von der Koalition gegen Stalkerware als Software definiert, die „die Überwachung von Intimpartnern sowie Belästigung, Missbrauch, Stalking und Gewalt begünstigen kann".

Das Ausmaß von digitaler Gewalt

Sieben von zehn Frauen in Europa, die von Cyberstalking betroffen waren, auch mindestens eine Form von körperlicher und/oder sexueller Gewalt durch einen Intimpartner erfahren.

Laut einem Bericht des Europäischen Instituts für Gleichstellungsfragen haben „sieben von zehn Frauen in Europa, die von Cyberstalking betroffen waren, auch mindestens eine Form von körperlicher und/oder sexueller Gewalt durch einen Intimpartner erfahren". In Anlehnung an diese Erkenntnisse betonen Experten von gemeinnützigen Organisationen, bei denen Überlebende und Opfer häuslicher Gewalt Unterstützung finden, dass auch Cyberstalking eine Form von Gewalt darstellt. Genau wie bei physischer, psychischer und sozioökonomischer Gewalt können Täter die Überwachung nutzen, um die vollständige Kontrolle über ihre Opfer[1] zu erlangen.

Durch die Verwendung von Stalkerware kann das Kontrollmaß des Täters immens sein. Je nach installiertem Produkt kann Stalkerware vielfältige Funktionen haben, um in die Privatsphäre der Betroffenen einzudringen. Mithilfe der Software kann ein Täter:

- alles lesen, was die überwachte Person eintippt, indem jede Tasteneingabe auf dem Gerät protokolliert wird – darunter auch die Anmeldedaten für Banking-Apps, Onlineshops und soziale Netzwerke.
- wissen, wo sich die betroffene Person befindet – durch Verfolgung der Bewegungen einer Person in Echtzeit via GPS.
- hören, was die Person sagt – durch Belauschen oder gar Aufzeichnen von Gesprächen.
- Nachrichten in jedem Messenger-Dienst lesen, unabhängig davon, ob eine Verschlüsselung verwendet wird.

1 Experten verwenden immer häufiger den ermächtigenden Begriff „Überlebende" statt „Opfer". Deshalb werden in diesem Bericht beide Begriffe verwendet.

- Aktivitäten in sozialen Netzwerken überwachen.
- Fotos und Videos ansehen.
- die Kamera einschalten.

All diese privaten Informationen können gesammelt werden, was in der Regel anhand eines Mobilgerätes, also ein Tablet oder ein Smartphone, erfolgt.

Gemeinnützige Organisationen der Koalition gegen Stalkerware verzeichnen eine wachsende Zahl von Betroffenen, die Hilfe zu diesem Problem benötigen.

Gemeinnützige Organisationen der Koalition gegen Stalkerware verzeichnen eine wachsende Zahl von Betroffenen, die Hilfe zu diesem Problem benötigen:

- Laut einer **australischen Studie** zu Technologiemissbrauch und häuslicher Gewalt, die von dem Women's Services Network (WESNET) mit Unterstützung von Dr. Delanie Woodlock und Forscherinnen und Forschern der Curtin University durchgeführt wurde, haben 99,3 % der Fachleute für häusliche Gewalt es mit Personen zu tun, die auch von technologiegestütztem Missbrauch betroffen sind. Der Einsatz von Videokameras ist dabei zwischen 2015 und 2020 um 183,2 % gestiegen.
- Laut einer Studie über Cybergewalt in intimen Beziehungen, die vom Centre Hubertine Auclert in **Frankreich** durchgeführt wurde, haben 21 % der Betroffenen den Einsatz von Stalkerware durch ihre/n missbrauchenden Partner bzw. Partnerin erlebt, und 69 % der Betroffenen haben das Gefühl, dass ihr Partner bzw. ihre Partnerin heimlich auf die persönlichen Daten auf ihrem Smartphone zugegriffen hat.
- In **Deutschland** beobachtet der Bundesverband Frauenberatungsstellen und Frauennotrufe (bff: Frauen gegen Gewalt) seit einigen Jahren eine zunehmende Nutzung von Stalkerware in Partnerschaftsbeziehungen.
- In den **USA** sind laut dem Stalking Prevention Awareness & Resource Center (SPARC) schätzungsweise 6 bis 7,5 Millionen Menschen innerhalb eines Jahres von Stalking betroffen. Jede vierte betroffene Person berichtet, durch irgendeine Form von Technologie gestalkt zu werden.

Physischer Zugriff ist der Schlüssel

Leider ist es nicht besonders schwierig, heimlich Stalkerware auf einem Smartphone zu installieren. Das größte Hindernis besteht darin, dass Stalkerware auf dem betroffenen Gerät konfiguriert werden muss. Aufgrund des Verbreitungsvektors solcher Anwendungen, der sich stark von den üblichen Verbreitungsschemata für Malware unterscheidet, ist es nicht möglich, sich über eine Spam-Nachricht mit einem Link zu Stalkerware oder durch eine Falle beim normalen Surfen im Internet mit Stalkerware zu infizieren.

Das bedeutet, dass der Täter (bzw. die Täterin) physischen Zugriff auf das Zielgerät haben muss, um Stalkerware zu installieren. Dies ist möglich, wenn das Gerät nicht durch eine PIN, ein Muster oder ein Passwort geschützt ist oder der Täter das Opfer

persönlich kennt. Die Installation auf dem Zielgerät kann innerhalb weniger Minuten abgeschlossen werden.

Vor dem Zugriff auf das Gerät muss der Täter einen Link zum Installationspaket von der Webseite des Stalkerware-Entwicklers abrufen. In den meisten Fällen wird die Software nicht von einem offiziellen App Store heruntergeladen. Für Android-Geräte hat Google Anwendungen, bei denen es sich eindeutig um Stalkerware handelt, seit 2020 aus seinem Play Store verbannt. Das bedeutet, dass Täter eine solche Anwendung nicht aus dem allgemeinen App Store installieren können. Stattdessen müssen sie mehrere Schritte befolgen, bevor die Stalkerware installieren werden kann. Deshalb kann es sein, dass Täter Spuren in den Geräteeinstellungen hinterlassen, die von den Betroffenen überprüft werden können, wenn sie den Verdacht haben, ausspioniert zu werden.

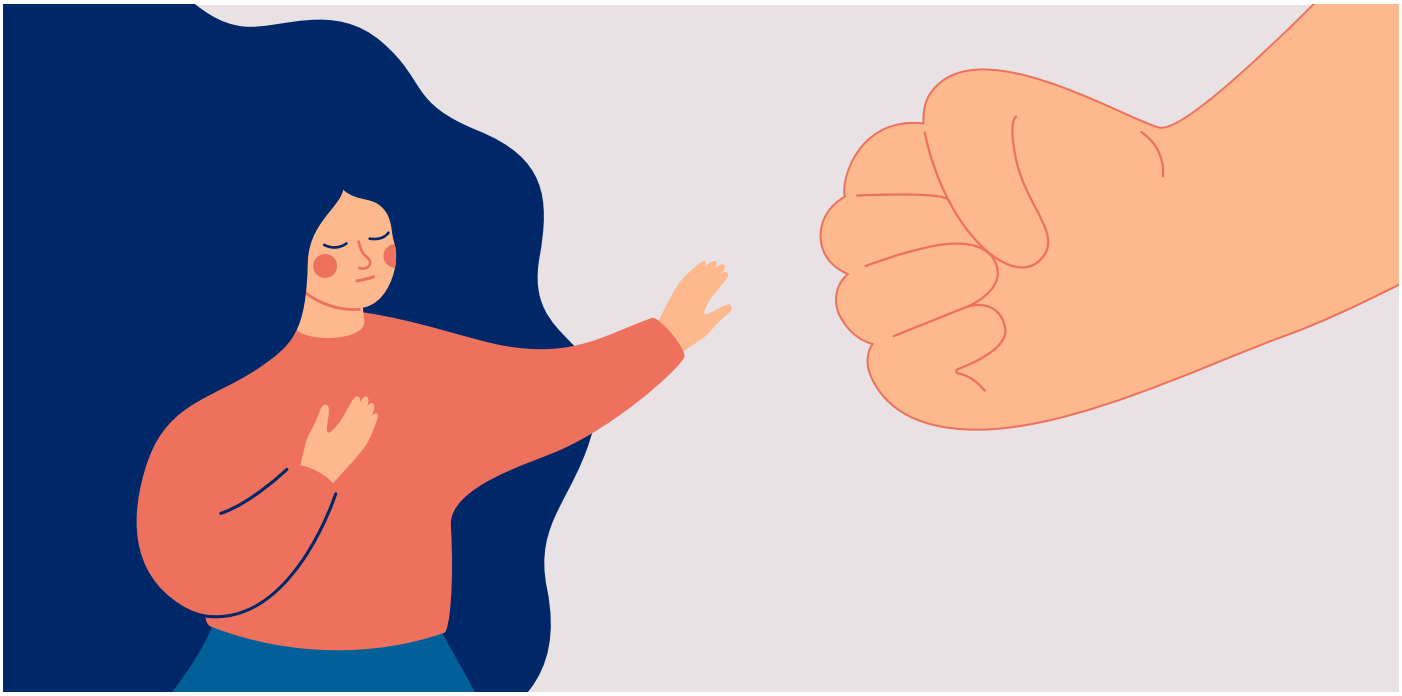
Stalkerware-Anwendungen sind auf iPhones seltener vorzufinden als auf Android-Geräten.

Stalkerware-Anwendungen sind auf iPhones seltener zu vorzufinden als auf Android-Geräten, da iOS traditionell ein geschlossenes System ist. Allerdings können Täter diese Einschränkung auf mittels Jailbreak freigeschalteten iPhones umgehen. Sie benötigen für die Freischaltung durch Jailbreak jedoch ebenfalls physischen Zugriff auf das Telefon. Zur Vermeidung einer unerwünschten Überwachung sollte man daher stets ein Auge auf das eigene Gerät haben. Alternativ können Täter ihrem Opfer ein iPhone – oder ein anderes Gerät – mit vorinstallierter Stalkerware als Geschenk überreichen. Es gibt einige Unternehmen, die diese Dienste zur Verfügung stellen, d.h. solche Tools auf einem neuen Smartphone installieren und als Geschenk in einer Originalverpackung an ahnungslose Adressaten liefern.

Das Risiko von Datenlecks

Informationen, die via Stalkerware abgefangen werden, stehen mindestens einer Person zur Verfügung – dem Täter, der die Stalkerware auf dem Smartphone der überwachten Person installiert hat. Es kommt jedoch auch vor, dass alle diese privaten Daten öffentlich zugänglich gemacht werden. Jahr für Jahr werden Stalkerware-Server entweder gehackt oder sie bleiben ungeschützt, sodass Informationen online abgerufen und weitergegeben werden können. Im Jahr 2020 kam es beispielsweise bei der Firma ClevGuard zu einem solchen Datenverstoß. In den vergangenen Jahren wurden ähnliche Vorfälle bei Mobiispy im Jahr 2019 und bei MSpy sowohl im Jahr 2018 als auch 2015 bekannt.

Dies sind nur einige Beispiele aus einer langen Liste, bei denen Datenbanken von Unternehmen, die Stalkerware entwickeln, offengelegt wurden und Millionen von Konten betroffen waren. Dabei ist die Möglichkeit, den Standort einer Person zu verfolgen, nicht nur ein Verlust ihrer Cyberprivatsphäre, sondern gefährdet auch die Sicherheit der überwachten Person in der realen Welt.



Die Rechtslage

Stalkerware-Anwendungen werden von Unternehmen unter einem Deckmantel verkauft und bereitgestellt, zum Beispiel als Lösungen für die Überwachung von Kindern oder zur Mitarbeiterkontrolle. Die Gesetze variieren zwar von Land zu Land, aber sie tragen dem Missbrauchspotenzial zunehmend Rechnung. Generell ist nur die Verwendung von Tools und Apps illegal, die Aktivitäten von Nutzern ohne deren Einwilligung oder anderweitige rechtliche Befugnis aufzeichnen. Allmählich zeichnen sich jedoch einige Änderungen in der Gesetzgebung ab. So hat Frankreich 2020 die Strafen für heimliche Überwachung verschärft: Die Ermittlung des geographischen Standorts von Personen („geolocating") ohne deren Einwilligung wird nun mit einem Jahr Haft und einer Geldstrafe von 45.000 Euro geahndet. Wenn dies innerhalb einer Paarbeziehung geschieht, sind die Sanktionen potenziell höher und können sich auf zwei Jahre Haft und eine Geldstrafe von 60.000 Euro belaufen.

Stalkerware-Tools verstoßen häufig gegen Gesetze; für Aufzeichnungen, die ohne das Wissen des Opfers erfolgt sind, können Haftungsansprüche gegen die Stalker geltend gemacht wurden. Einem Stalker muss klar sein, dass er allein gegen das Gesetz verstößt. Wenn der Einsatz von Stalkerware gemeldet wird, wird die Privatperson strafrechtlich belangt, die die Software installiert hat – nicht der Hersteller. In den USA wurden in der jüngeren Geschichte nur zwei Entwickler von Stalking-Apps zu Geldstrafen verurteilt. In einem Fall wurde eine Rekordstrafe von 500.000 US-Dollar fällig, infolgedessen wurde die Entwicklung der App eingestellt. Im anderen Fall blieb es bei einer Anordnung, die wFunktionalität der App für den zukünftigen Vertrieb zu ändern.

Das Ausmaß des Problems

Globale Erkennungszahlen – betroffene Nutzer

Die Zahl der Betroffenen ist nach wie vor hoch. Insgesamt waren im Jahr 2020 weltweit 53.870 individuelle Nutzer von Stalkerware betroffen. Im Vergleich dazu waren es im Jahr 2019 weltweit 67.500 individuelle Nutzer.

In diesem Abschnitt betrachten wir die Gesamtzahl der individuellen Nutzer, auf deren Mobilgerät Stalkerware erkannt wurde.

Die Daten für 2020 zeigen, dass sich die Stalkerware-Situation nicht wesentlich verbessert hat: Die Zahl der Betroffenen ist nach wie vor hoch. Insgesamt waren im Jahr 2020 weltweit 53.870 individuelle Nutzer von Stalkerware betroffen. Im Vergleich dazu waren es im Jahr 2019 weltweit 67.500 individuelle Nutzer. Man muss jedoch die Tatsache berücksichtigen, dass 2020 ein beispielloses Jahr war, in dem sich das Leben auf der ganzen Welt auf dramatische Weise verändert hat.

Zur Eindämmung der COVID-19-Pandemie wurden in allen Ländern der Welt massive Einschränkungen wie Maßnahmen zur Selbstisolierung oder Lockdowns veranlasst. Wenn man bedenkt, dass Stalkerware als ein zusätzliches Tool eingesetzt wird, um eine/n im gleichen Haushalt lebende/n Intimpartner bzw. Intimpartnerin im Alltag zu kontrollieren, kann dies eine Erklärung für die etwas niedrigeren Zahlen im Vergleich zum Vorjahr sein.

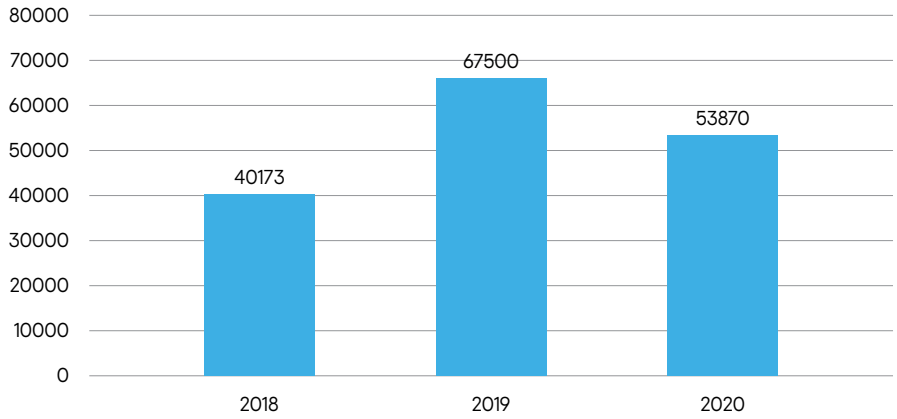


Tabelle 1 Von Stalkerware betroffene Nutzer weltweit von 2018 bis 2020 – Gesamtzahl pro Jahr

Dennoch sind die Zahlen für 2020 immer noch auf einem hohen, stabilen Niveau. Im Vergleich dazu wurden im Jahr 2018 weltweit 40.173 individuelle Nutzer erfasst, die von Stalkerware betroffen waren.

Wenn man sich die Gesamtzahlen der weltweit von Stalkerware betroffenen Nutzer im Jahr 2020 pro Monat ansieht, wird dieser Trend noch deutlicher. In den ersten beiden Monaten des Jahres gab es eine hohe Anzahl an betroffener Geräte, was zeigt, dass Stalkerware ziemlich stark verbreitet war. Die Situation änderte sich im März, als viele Länder beschlossen, Quarantänemaßnahmen zu verhängen. Die Kurve zeigt einen Trend, wonach sich die Zahlen ab Juni 2020, als viele Länder auf der Welt die Beschränkungen lockerten, allmählich wieder stabilisierten.

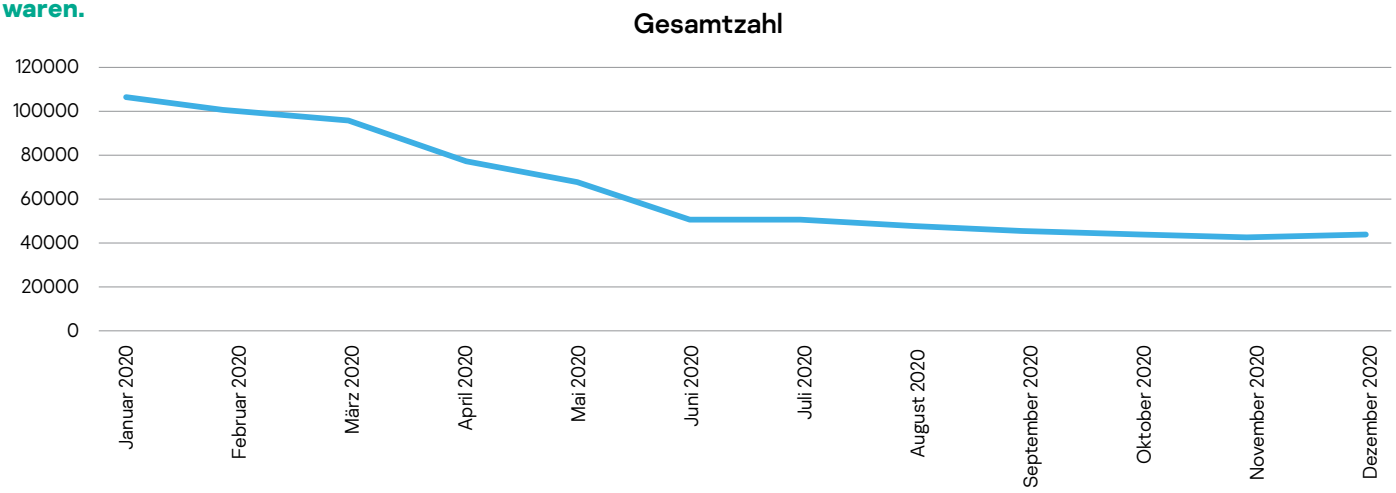


Tabelle 2 Von Stalkerware betroffene individuelle Nutzer im Jahr 2020 weltweit – Gesamtzahl nach Monat

Dennoch sind die Zahlen für 2020 immer noch auf einem hohen, stabilen Niveau. Im Vergleich dazu wurden im Jahr 2018 weltweit 40.173 individuelle Nutzer erfasst, die von Stalkerware betroffen waren. Dies relativiert die Gesamtzahlen aus dem Jahr 2020, da wir eine zunehmende Integration von Technologie in unser Leben erlebt haben. Leider bedeutet dies auch, dass die für Stalking verwendete Software als eine weitere Form der Gewalt in der Partnerschaft immer häufiger zum Einsatz kommt.

Globale Erkennungszahlen – Stalkerware-Programme

In diesem Abschnitt analysieren wir, welche Stalkerware-Programme weltweit tatsächlich am häufigsten für die Kontrolle von Mobilgeräten verwendet werden. Die folgenden Ergebnisse geben Aufschluss über die im Jahr 2020 am häufigsten erkannten Programme

	Programme	Betroffene Nutzer
1	Monitor.AndroidOS.Nicb.a	8147
2	Monitor.AndroidOS.Cerberus.s	5429
3	Monitor.AndroidOS.Agent.af	2727
4	Monitor.AndroidOS.Anlost.a	2234
5	Monitor.AndroidOS.MobileTracker.c	2161
6	Monitor.AndroidOS.PhoneSpy.b	1774
7	Monitor.AndroidOS.Agent.hb	1463
8	Monitor.AndroidOS.Cerberus.a	1310
9	Monitor.AndroidOS.Reptilic.a	1302
10	Monitor.AndroidOS.SecretCam.a	1124

Tabelle 3 – Top 10 der weltweit im Jahr 2020 am häufigsten entdeckten Stalkerware-Programme

1. Mit mehr als 8.100 betroffenen Nutzern war **Nidb** das meistgenutzte Stalkerware-Programm im Jahr 2020. Der Hersteller von Nidb verkauft sein Produkt als „Stalkerware-as-a-Service". Das bedeutet, dass jede Person die Kontrollserversoftware und mobile App des Herstellers mieten und unter eigenem Namen verkaufen könnte – Beispiele hierfür sind iSpyoo, TheTruthSpy, Copy9 und andere.
2. Der zweite und der achte Platz werden von Cerberus belegt. Es handelt sich um zwei Programme aus derselben Familie. Von der Variante **Cerberus.a** waren mehr als 5.400 Nutzer betroffen.
3. An dritter Stelle steht **Agent.af**, von dem mehr als 2.700 Nutzer betroffen waren. Diese wird als „Track My Phone" vermarktet und verfügt über typische Funktionen wie das Auslesen von Nachrichten aus beliebigen Messengern, die Protokollierung der Anrufliste einer Person und die Verfolgung einer Person via Geolokalisierung.
4. **Anlost.a** ist ein klares Beispiel für „getarnte" Stalkerware. Sie wird als App für Diebstahlschutz beworben und ihr Symbol ist auf dem Startbildschirm sichtbar (kein übliches Verhalten für getarnte Stalkerware-Apps). Daher ist sie im Google Play Store verfügbar. Es ist jedoch möglich, das Symbol auf dem Startbildschirm auszublenden. Eine der Hauptfunktionen der Anwendung ist das Abfangen von SMS-Nachrichten und das Auslesen des Anrufprotokolls. Mehr als 2.200 Nutzer waren von diesem Programm betroffen.
5. **MobileTracker.c** verfügt über vielfältige Funktionen, wie z. B. das Abfangen von Nachrichten aus beliebten sozialen Netzwerken und die Fernsteuerung des betroffenen Geräts. Mehr als 2.100 Nutzer waren von diesem Programm betroffen.
6. **PhoneSpy** ist auch als Spy Phone App oder Spapp Monitoring bekannt. Diese Anwendung besteht aus vielen Ausspähfunktionen, die alle gängigen Instant Messenger und sozialen Netzwerke abdecken.
7. **Agent.hb** ist eine weitere Version von MobileTracker. Wie die Originalversion bietet dieses Programm vielfältige Funktionen.
8. **Cerberus.b**, eine weiteres Programm aus derselben Familie wie Cerberus.a.
9. **Reptilic.a** ist Stalkerware, die vielfältige Funktionen wie die Überwachung sozialer Medien, Anrufaufzeichnungen und die Überwachung des Browserverlaufs enthält.
10. **SecretCam**.a ist eine Kamera-Stalking-Software, d. h. sie ist in der Lage, heimlich Videos von der vorderen oder hinteren Kamera des betroffenen Geräts aufzunehmen.

Geografische Verteilung der betroffenen Nutzer

Stalkerware ist ein globales Phänomen, das Länder unabhängig von ihrer Größe, Gesellschaft oder Kultur betrifft. Betrachtet man die Top 10 der weltweit betroffenen Länder im Jahr 2020, so zeigen die Ergebnisse von Kaspersky, dass weitgehend dieselben Länder am stärksten betroffen bleiben, mit Russland an erster Stelle. Allerdings konnten wir 2020 im Vergleich zu 2019 einen Anstieg der Stalkerware-Aktivitäten in Brasilien und den USA beobachten. Wir haben jedoch weniger Vorfälle in Indien festgestellt, was somit in der Rangliste zurückgefallen ist. Außerdem haben wir eine höhere Anzahl von Vorfällen in Mexiko festgestellt, das in der Rangliste um zwei Plätze aufgestiegen ist.

	Land	Betroffene Nutzer
1	Russische Föderation	12.389
2	Brasilien	6.523
3	USA	4.745
4	Indien	4.627
5	Mexiko	1.570
6	Deutschland	1.547
7	Iran	1.345
8	Italien	1.144
9	Vereinigtes Königreich (UK)	1.009
10	Saudi-Arabien	968

Tabelle 4 – Top 10 der weltweit am häufigsten von Stalkerware betroffenen Länder im Jahr 2020 – weltweit

In Europa sind Deutschland, Italien und UK in dieser Reihenfolge die drei am stärksten betroffenen Länder. Es folgen Frankreich auf dem vierten und Spanien auf dem fünften Platz.

	Land	Betroffene Nutzer
1	Deutschland	1.547
2	Italien	1.144
3	Vereinigtes Königreich (UK)	1.009
4	Frankreich	904
5	Spanien	873
6	Polen	444
7	Niederlande	321
8	Rumänien	222
9	Belgien	180
10	Österreich	153

Tabelle 5 – Top 10 der weltweit am häufigsten von Stalkerware betroffenen Länder im Jahr 2020 – Europa

Ist auf meinem Mobilgerät Stalkerware installiert?

Für Laien ist schwer zu erkennen, ob Stalkerware auf ihrem Gerät installiert ist. In der Regel bleibt diese Art von Software verborgen. Das bedeutet auch, dass das Symbol der Stalkerware-App auf dem Startbildschirm und im Telefonmenü ausgeblendet wird und alle digitalen Spuren „beseitigt" werden. Sie kann sich jedoch verraten und es gibt einige Warnzeichen. Orientieren bieten dabei folgende Anhaltspunkte:

- Achten Sie auf einen sich schnell entleerenden Akku, ständige Überhitzung und zunehmenden mobilen Datenverkehr.
- Führen Sie regelmäßig einen Antiviren-Scan auf Ihrem Android-Gerät durch: Wenn die Cybersicherheitslösung Stalkerware entdeckt hat, sollten Sie **diese nicht überstürzt entfernen, da der Täter bzw. die Täterin dies bemerken könnte**. Halten Sie einen Sicherheitsplan bereit und wenden Sie sich an eine lokale Hilfsorganisation.
- Prüfen Sie den Browserverlauf: Um Stalkerware herunterzuladen, muss der Täter bzw. die Täterin einige Webseiten besuchen, die die betroffene Person nicht kennt. Alternativ könnte es überhaupt keine Verlaufsdaten geben, wenn sie infolge des Missbrauchs gelöscht wurden.
- Prüfen Sie die Einstellung der Sicherheits-Option „Unbekannte Herkunft" (auch: „Unbekannte Quellen"): Wenn auf Ihrem Gerät diese Option aktiviert ist, könnte dies ein Zeichen dafür sein, dass unerwünschte Software aus einer fremden Quelle installiert wurde.
- Überprüfen Sie die Berechtigungen der installierten Apps: Die Stalkerware-App kann zur Tarnung einen falschen Namen tragen und verdächtigen Zugriff auf Nachrichten, Anrufprotokolle, Standort und andere persönliche Aktivitäten gewähren.

Es ist jedoch auch wichtig zu verstehen, dass solche Warnzeichen oder Symptome nicht unbedingt ein Beweis dafür sind, dass Stalkerware auf einem Gerät installiert ist.

So minimieren Sie das Risiko

Im Zusammenhang mit häuslicher Gewalt und Missbrauch in Beziehungen kann es schwierig oder sogar unmöglich sein, den Zugang zum mobilen Gerät zu verweigern.

Es gibt Möglichkeiten, um die digitale Sicherheit zu erhöhen:

- Leihen Sie Ihr Smartphone niemals an andere Personen aus, ohne sehen zu können, was damit passiert, und lassen Sie es nirgendwo entsperrt liegen.*
- Verwenden Sie ein komplexes Passwort für die Bildschirmsperre und ändern Sie Passwörter in regelmäßigen Abständen.
- Geben Sie Ihr Passwort an niemanden weiter – auch nicht an Intimpartner/in, Familienmitglieder oder enge Freunde.*
- Überprüfen Sie Ihr Telefon regelmäßig – löschen Sie Apps, die Sie nicht verwenden, und prüfen Sie die Berechtigungen für jede App.
- Deaktivieren Sie die Option zur Installation von Drittanbieter-Anwendungen auf Android-Geräten.
- Schützen Sie Ihre Android-Geräte mit einer Cybersicherheitslösung wie Kaspersky Internet Security for Android (kostenlos erhältlich), die Stalkerware erkennt und Sie im Ernstfall benachrichtigt.

*Im Zusammenhang mit häuslicher Gewalt und Missbrauch in Beziehungen kann es schwierig oder sogar unmöglich sein, den Zugang zum mobilen Gerät zu verweigern.

Kasperskys Beitrag zur Bekämpfung von digitaler Gewalt

Kaspersky arbeitet aktiv daran, digitale Gewalt und dem Missbrauch von Stalkerware Einhalt zu gebieten – sowohl als Unternehmen als auch gemeinsam mit vielen anderen Partnern. Im Jahr 2019 haben wir eine spezielle Warnmeldung entwickelt, die Nutzer benachrichtigt, wenn Stalkerware auf ihren Telefonen installiert wurde. Im selben Jahr haben wir mit neun weiteren Akteuren aus Wirtschaft und Gesellschaft die Koalition gegen Stalkerware gegründet. Im Jahr 2020 haben wir TinyCheck entwickelt, ein kostenloses Tool zur Erkennung von Stalkerware auf Mobilgeräten. Die Anwendung richtet sich speziell an gemeinnützige Organisationen, die mit Betroffenen häuslicher Gewalt arbeiten. TinyCheck finden Sie unter https://github.com/KasperskyLab/TinyCheck. Seit 2021 sind wir zudem einer von fünf Partnern in einem EU-weiten Projekt zur Bekämpfung von geschlechtsspezifischer digitaler Gewalt und Stalkerware namens „DeStalk“, das die Europäische Kommission mit ihrem Programm „Rechte, Gleichstellung und Unionsbürgerschaft“ gefördert hat.

Über die Koalition gegen Stalkerware

Die Koalition gegen Stalkerware (Coalition against Stalkerware, CAS) ist eine Gruppe, die sich der Bekämpfung von Missbrauch, Stalking und Belästigung durch die Entwicklung und Verwendung von Stalkerware widmet. Die im November 2019 gestartete Koalition gegen Stalkerware hat in ihrem ersten Jahr 26 Partner gewonnen. Dazu gehören die Gründungsmitglieder Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA Cyber Defense, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape und WEISSER RING. Die Koalition möchte eine Vielzahl von Organisationen zusammenbringen, um aktiv gegen kriminelle Machenschaften auf Basis von Stalkerware vorzugehen und das öffentliche Bewusstsein für dieses wichtige Thema zu schärfen. Aufgrund der hohen gesellschaftlichen Relevanz für Menschen auf der ganzen Welt und regelmäßig neu auftauchender Varianten von Stalkerware ist die Koalition gegen Stalkerware offen für neue Partner und ruft zur Zusammenarbeit auf. Weitere Informationen über die Koalition gegen Stalkerware finden Sie auf der offiziellen Website www.stopstalkerware.org/de.